

Annual 47 C.F.R. § 64.2009(e) CPNI Certification

EB Docket 06-36

Annual 64.2009(e) CPNI Certification for 2019 covering the prior calendar year, 2018.

Date filed: March 7, 2019

Name of company (ies) covered by this certification: U.S. TelePacific Corp., TPx Communications Co., Mpower Communications Corp., Arrival Communications, Inc. and DSCI, LLC, all d/b/a TPx Communications Co. (collectively referred to herein as "the Company").

Form 499 Filer IDs: 819502/825412/817290/803442/821296

Name of signatory: William Hunt

Title of signatory: Senior Vice President, General Counsel and Secretary

Certification:

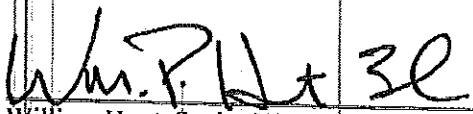
I, William Hunt, certify that I am an officer of the Company named above, and acting as an agent of the Company, that I have personal knowledge that the Company has established operating procedures that are adequate to ensure compliance with the Commission's CPNI rules. See 47 C.F.R. § 64.2001 *et seq.*

Attached to this certification is an accompanying statement explaining how the Company's procedures ensure that the Company is in compliance with the requirements (including those mandating the adoption of CPNI procedures, training, recordkeeping, and supervisory review) set forth in section 64.2001 *et seq.* of the Commission's rules. Statement attached.

The Company has not taken actions (i.e. proceedings instituted or petitions filed by a company at state commissions, the court system or the Commission) against data brokers in the past year.

The Company received no direct customer complaints in the past year concerning the unauthorized release of CPNI.

The Company represents and warrants that the above certification is consistent with 47 C.F.R. Sec. 1.17 which requires truthful and accurate statements to the Commission. The Company also acknowledges that false statements and misrepresentations to the Commission are punishable under Title 18 of the U.S. Code and may subject it to enforcement action.



William Hunt, Senior Vice President, General Counsel and Secretary

Supporting Statement re CPNI Procedures
TPx Communications Co. Companies

- U.S. TelePacific Corp. d/b/a TPx Communications (“TPx” or “Company”) have mandated procedures for verifying that the Call Center, Repair and other customer-facing personnel are providing CPNI only to authorized customers and users.
 - TPx instituted strict procedures for matching callers with authorized user information in its databases and for calling out to main telephone numbers to contact authorized users, when needed.
 - TPx initially instituted manually-signed customer forms for authorization to use or change customer information, whether by internal customer representatives or on an on-going basis by agents of customers. TPx has subsequently modified these forms slightly for enhanced efficiency.
 - Forms initially were made available electronically and returnable, signed & on letterhead, by fax, e-mail, or mail. These are now back-up systems.
 - TPx subsequently completed the development and implementation of automated e-mail confirmations of all changes to customer account information. More specifically, when talking to an authorized user who desires to update and/or change customer information, a pre-formatted e-mail can be completed & sent to an authorized user, with “voting buttons,” to return the e-mail with a confirmation, or denial, of change. These documents are automatically retained in company databases.
 - TPx has actively sought updated or expanded information regarding authorized users, when in contact with an authorized user, and now “flags” accounts for which authorized user information has not been confirmed within the past six months.
 - Fraud control procedures provide for investigation of any automated e-mail confirmation which results in a denial of change.
- On-Line Systems: Password-related procedures for TPx on-line systems were upgraded to ensure they meet all aspects of the rules.
- When customer online databases are consolidated, customers are required to meet more restrictive password requirements and provide security questions.
- An authorized user is automatically notified of any account changes.

- Training: Extensive, required initial training sessions were held. Additional training sessions have been held on system upgrades such as the automated e-mails. An explanation of basic CPNI requirements is provided on-line and in various documents, including the Employee Guidebook, "mini-training" for all new employees, the anti-fraud presentation made to all new sales personnel, as well as periodic CPNI awareness "Flashes," for example, when issues arise that merit special attention.
- TPx has expanded and up-graded its training programs with the intent of assuring in depth and detailed new hire training for customer-facing personnel. These and other materials are also available on the TPx intranet so employees can refresh their recollection or find answers to CPNI questions at any time.
- Marketing: TPx has long had required policies and procedures regarding use of CPNI for marketing, including supervisory review and record retention.
- Breach Procedures: Breach prevention and response procedures were reviewed for completeness & effectiveness and company has established more detailed procedures for meeting any potential breach more quickly and efficiently.
- TPx also developed procedures to allow for automated database retention and automated searches for reported breach-related information.
- Security Upgrade Efforts: TPx has evaluated the best means of providing secure/encrypted laptops to employees. A limited number of full encryption laptops have been provided to date and IT is continuing to study and evaluate the most efficient and cost effective means of assuring that most employees, particularly those who tend to take their laptops out of the office, will have secure laptops within a reasonable period of time.
- Oversight & Review: In addition, to assure that all customer confidential information is protected, whether it is voice or data information, TPx instituted an oversight and development committee to review procedures regarding processes related to protecting customer confidential information and to see that those processes are upgraded periodically as appropriate.